



## OPINION OF THE EUROPEAN CENTRAL BANK

of 25 July 2014

**on a proposal for a directive of the European Parliament and of the Council concerning measures to ensure a high common level of network and information security across the Union (CON/2014/58)**

### **Introduction and legal basis**

On 7 February 2013, the European Commission published a proposal for a directive concerning measures to ensure a high common level of network and information security across the Union<sup>1</sup> (hereinafter the ‘proposed directive’).

The European Central Bank (ECB) has decided to deliver an own initiative opinion on the proposed directive, since it has not been formally consulted by the legislators. The ECB’s competence to deliver an opinion is based on Articles 127(4) and 282(5) of the Treaty on the Functioning of the European Union since the proposed directive contains provisions affecting the task of the European System of Central Banks (ESCB) to promote the smooth operation of payment systems as referred to in the fourth indent of Article 127(2) of the Treaty. In addition, Article 22 of the Statute of the European System of Central Banks and of the European Central Bank (hereinafter the ‘Statute of the ESCB’) provides that the ECB and national central banks (NCBs) may provide facilities, and the ECB may make regulations, to ensure efficient and sound clearing and payment systems within the Union and with other countries. In accordance with the first sentence of Article 17.5 of the Rules of Procedure of the European Central Bank, the Governing Council has adopted this opinion.

### **1. Purpose of the proposed directive**

1.1 The proposed directive aims to ensure a high common level of network and information security (NIS) by improving the security of the internet and the network and information systems which underpin our society and the economy. This proposal is the main action under the European Cybersecurity Strategy<sup>2</sup>.

---

<sup>1</sup> COM (2013) 48 final.

<sup>2</sup> See Joint Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, ‘Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace’, [JOIN \(2013\) 1 final](#).

## ECB-PUBLIC

- 1.2 Network and information systems play an essential role in facilitating the cross-border movement of goods, services and people. Given this intrinsic transnational dimension, a disruption in one Member State can also affect other Member States and the Union as a whole. In addition, the likelihood that incidents will frequently occur and the inability to ensure efficient protection undermine public trust and confidence in NIS. The resilience and stability of NIS is therefore critical to the smooth functioning of the internal market.
- 1.3 The proposed directive builds on previous initiatives in this area. Against this background, the proposed directive recognises the need to harmonise rules on NIS and to create effective cooperation mechanisms among the Member States<sup>3</sup>.
- 1.4 The proposed directive establishes a common Union legal framework for NIS regarding Member States' capabilities, mechanisms for Union-level cooperation and requirements for public administrations and also private sector entities in specified critical sectors. This should ensure adequate preparedness at national level and help foster a climate of mutual trust, which is a precondition for effective cooperation at Union level. Setting up mechanisms for cooperation at Union level via the network will deliver a coherent and coordinated means of preventing and responding to cross-border NIS incidents and risks.
- 1.5 The main provisions concern the following:
- (a) a requirement that all Member States have a minimum level of national capabilities in place by establishing competent authorities for NIS, setting up Computer Emergency Response Teams (CERTs) and adopting national NIS strategies and national NIS cooperation plans;
  - (b) mandated information sharing between Member States within a network, as well the creation of a pan-European NIS cooperation plan and coordinated early warnings for cyber-security incidents;
  - (c) based on the model of Directive 2002/21/EC of the European Parliament and of the Council<sup>4</sup>, ensuring that a culture of risk management develops and that information is shared between the private and public sectors. Companies in the specific critical sectors and public administrations will be required to assess the risks they face and adopt appropriate and proportionate measures to ensure NIS. They will also be required to report to the competent authorities any incidents seriously compromising their networks and information systems and significantly affecting the continuity of critical services and supply of goods.

---

<sup>3</sup> These include the following communications: 'Network and Information Security: Proposal for a European Policy Approach' COM (2001) 298 final; 'A strategy for a Secure Information Society: "Dialogue, partnership and empowerment"' COM(2006) 251 final; 'Critical Information Infrastructure Protection – "Protecting Europe from large scale cyber-attacks and disruptions: enhancing preparedness, security and resilience"' COM(2009) 149 final; 'A Digital Agenda for Europe' COM(2010) 245 final; and 'Critical Information Infrastructure Protection – "Achievements and next steps: towards global cyber-security"' COM(2011) 163 final.

<sup>4</sup> Directive 2002/21/EC of the European Parliament and of the Council of 7 March 2002 on a common regulatory framework for electronic communications networks and services (OJ L 108, 24.4.2002, p. 33).

## 2 General observations

- 2.2 The ECB supports the aim of the proposed directive to ensure a high common level of NIS across the Union and to achieve a consistency of approach in this area across business sectors and Member States. It is important to ensure that the internal market is a safe place to do business and that all Member States have a certain minimum level of preparedness in the case of a cyber-security incident.
- 2.3 However, the ECB considers that the proposed directive should be without prejudice to the existing regime for the Eurosystem's oversight of payment and settlement systems<sup>5</sup>, which includes appropriate arrangements, inter alia, in the area of NIS. It should be noted that the ECB has a particular interest in enhanced security in payment and settlement<sup>6</sup> systems in order to promote the smooth operation of payment systems and help maintain confidence in the euro and the functioning of the economy in the Union.
- 2.4 Furthermore, the assessment of security arrangements and incident notifications for payment and settlement systems and payment service providers (PSPs) is one of the core competences of prudential supervisors and central banks. Responsibility for developing oversight requirements in the abovementioned areas should therefore remain with these authorities, and should not be subject to potentially conflicting requirements imposed by other national authorities. Furthermore, risk management, including security requirements in respect of payment and settlement systems and other market infrastructures within the euro area, is set by the Eurosystem, comprising the ECB and NCBs from those Member States that have adopted the euro. Through this oversight function, the Eurosystem aims to ensure the smooth functioning of payment and settlement systems by applying, inter alia, appropriate oversight standards and minimum requirements. The proposed directive should take into account the oversight framework already in place and ensure regulatory consistency across the Union.

## 3 Specific observations

- 3.1 Recital 5 and Article 1 of the proposed directive provide that the relevant obligations, cooperation mechanism and security requirements shall apply to all public administrators and market operators. The current wording of recital 5 and Article 1 does not take into account the Eurosystem's mandate, enshrined in the Treaty, to oversee payment and settlement systems. The proposed directive should therefore be amended to properly reflect the Eurosystem's responsibilities in this area.

---

<sup>5</sup> The oversight functions of some ESCB members are carried out on the basis of national laws and regulations, which complement, and in some cases duplicate, the Eurosystem's competence.

<sup>6</sup> The term 'settlement' as used throughout this opinion includes the clearing function.

3.2 The arrangements and procedures for central banks and other competent authorities to oversee payment and securities settlement systems are contained in a number of Union directives and regulations including, in particular:

- (a) Directive 98/26/EC of the European Parliament and of the Council (hereinafter ‘the Settlement Finality Directive’)<sup>7</sup>, which entitles the competent authorities of Member States to impose supervisory arrangements on payment and settlement systems which fall under their jurisdiction<sup>8</sup>;
- (b) Regulation (EU) No 648/2012 of the European Parliament and of the Council<sup>9</sup> (hereinafter the ‘European Market Infrastructure Regulation’ (EMIR)), which recognises the roles of the European Securities and Markets Authority (ESMA), the European Banking Authority (EBA) and the ESCB in setting regulatory standards and supervising central counterparties; and
- (c) the proposal for a Regulation on improving securities settlement in the European Union and on central securities depositories (CSDs) and amending Directive 98/26/EC<sup>10</sup> (hereinafter the ‘CSD Regulation’ (CSDR)), which identifies the competent authorities to be vested with supervisory and investigatory powers, and in particular Article 45 of that regulation, which introduces prudential requirements for the CSDs, including important provisions on the mitigation of operational risk.

3.3 Moreover, it should be noted that, on 3 June 2013, the ECB’s Governing Council adopted the ‘Principles for financial market infrastructures’, introduced in April 2012 by the Committee on Payment and Settlement Systems (CPSS) of the Bank for International Settlements and the Technical Committee of the International Organization of Securities Commissions (IOSCO)<sup>11</sup>, for the conduct of Eurosystem oversight in relation to all types of financial market infrastructures. This was followed by a public consultation regarding a draft regulation on oversight requirements for systemically important payment systems (hereinafter the ‘SIPS Regulation’)<sup>12</sup>. The SIPS Regulation implements the CPSS-IOSCO principles in a legally binding way and covers both large-value and retail payment systems of systemic importance, whether operated by Eurosystem NCBs or private entities.

---

<sup>7</sup> Directive 98/26/EC of the European Parliament and of the Council of 19 May 1998 on settlement finality in payment and securities settlement systems (OJ L 166, 11.6.1998, p. 45).

<sup>8</sup> Please see the third subparagraph of Article 10(1) of the Settlement Finality Directive.

<sup>9</sup> Regulation (EU) No 648/2012 of the European Parliament and of the Council of 4 July 2012 on OTC derivatives, central counterparties and trade repositories (OJ L 201, 27.7.2012, p. 1).

<sup>10</sup> COM (2012) 73 final.

<sup>11</sup> Available on the Bank of International Settlements website at <https://www.bis.org/publ/cpss94.pdf>.

<sup>12</sup> Available on the ECB website at <http://www.ecb.europa.eu>.

## ECB-PUBLIC

- 3.4 The existing oversight arrangements<sup>13</sup> in respect of payment systems and PSPs already contain procedures for early warnings<sup>14</sup> and coordinated responses<sup>15</sup> within and beyond the Eurosystem to deal with possible cyber-security threats, which are equivalent to those laid down in Articles 10 and 11 of the proposed directive.
- 3.5 The ESCB has set standards regarding reporting and risk management obligations for payment systems. Furthermore, the ECB regularly assesses securities settlement systems in order to determine their eligibility for use in the Eurosystem credit operations. Therefore, the ECB considers it necessary that the requirements in the proposed directive affecting critical market infrastructures and their operators<sup>16</sup> do not prejudice the standards in the SIPS Regulation, the Eurosystem's oversight policy framework or other Union regulations, and in particular EMIR and the future CSDR. Moreover, it should not interfere with the tasks of the EBA or ESMA and other prudential supervisors<sup>17</sup>.
- 3.6 Notwithstanding the above, the ECB considers that there is a strong case for the Eurosystem to share relevant information with the NIS Committee to be set up pursuant to Article 19 of the proposed directive. For purposes of effective information sharing that may become necessary, the ECB, EBA and ESMA should be invited to send representatives to meetings of the NIS Committee for agenda items which could be of interest for the performance of their respective mandates.

Done at Frankfurt am Main, 25 July 2014.

[signed]

*The President of the ECB*

Mario DRAGHI

---

<sup>13</sup> See the ECB's press release regarding the Memorandum of Understanding (MoU) on high-level principles of cooperation between the banking supervisors and central banks of the European Union in crisis management situations (2003), available on the ECB's website at [www.ecb.europa.eu](http://www.ecb.europa.eu).

<sup>14</sup> See Recommendation 3: incident monitoring and reporting in 'Recommendations for the security of internet payments-final version after public consultation', The European Forum on the Security of Retail Payments (SecuRe Pay), January 2013, available on the ECB's website at [www.ecb.europa.eu](http://www.ecb.europa.eu).

<sup>15</sup> Based on the principles for cooperative international oversight, as reiterated by the CPSS oversight report of 2005, Eurosystem central banks have participated successfully in cooperative arrangements in a number of cases, as shown, for example, in the context of the oversight arrangements for SWIFT (the Society for Worldwide Interbank Financial Telecommunications) and for Continuous Linked Settlement (CLS).

<sup>16</sup> For example, the requirements for market operators to observe technical and organisational measures in Articles 14(3) and (4) and the power to issue binding instructions to market operators in Article 15(3) of the proposed directive .

<sup>17</sup> See page 6 of the ECB Opinion on a proposal for a directive of the European Parliament and of the Council on payment services in the internal market and amending Directives 2002/65/EC, 2013/36/EU and 2009/110/EC and repealing Directive 2007/64/EC (CON/2014/9). All ECB opinions are published on the ECB's website at [www.ecb.europa.eu](http://www.ecb.europa.eu).

**Drafting proposals**

<b>Text proposed by the Commission</b>	<b>Amendments proposed by the ECB<sup>1</sup></b>
Amendment 1	
Recital 5	
<p>‘(5) To cover all relevant incidents and risks, this Directive should apply to all network and information systems. The obligations on public administrations and market operators should however not apply to undertakings providing public communication networks or publicly available electronic communication services within the meaning of Directive 2002/21/EC of the European Parliament and of the Council of 7 March 2002 on a common regulatory framework for electronic communications networks and services (Framework Directive)<sup>2</sup>, which are subject to the specific security and integrity requirements laid down in Article 13a of that Directive nor should they apply to trust service providers.’</p>	<p>‘(5) To cover all relevant incidents and risks, this Directive should apply to all network and information systems. The obligations on public administrations and market operators should however not apply to undertakings providing public communication networks or publicly available electronic communication services within the meaning of Directive 2002/21/EC of the European Parliament and of the Council of 7 March 2002 on a common regulatory framework for electronic communications networks and services (Framework Directive)<sup>2</sup>, which are subject to the specific security and integrity requirements laid down in Article 13a of that Directive nor should they apply to trust service providers. <b>Furthermore, notwithstanding the application of this Directive to public administrations and market operators, this Directive does not affect the tasks and duties conferred on the European System of Central Banks (ESCB) by the Treaty and the Statute of the European System of Central Banks and of the European Central Bank, nor equivalent functions performed by ESCB members under their national</b></p>

<sup>1</sup> Bold in the body of the text indicates where the ECB proposes inserting new text. Strikethrough in the body of the text indicates where the ECB proposes deleting text.

	<p><b>frameworks, especially regarding policies relating to the prudential supervision of credit institutions and the oversight of payment and securities settlement systems. Member States shall rely on the prudential supervision and oversight functions exercised by the central banks and supervisors of such operators within their fields of competence.’</b></p>
<p style="text-align: center;"><u>Explanation</u></p> <p><i>Recital 5 should be amended in order to reflect the responsibilities of the ECB and the NCBs in overseeing and regulating payment and settlement systems. Pursuant to the fourth indent of Article 127(2) of the Treaty, one of the core tasks of the ESCB is to promote the smooth operation of payment systems. Article 22 of the Statute of the ESCB also empowers the ECB to make regulations to ensure efficient and sound clearing and payment systems. It should also be taken into consideration that, under Article 127(5) of the Treaty, the ESCB shall contribute to the smooth conduct of policies relating to the stability of the financial system. Furthermore, according to the Eurosystem’s Oversight Policy Framework of July 2011<sup>2</sup>, the ‘oversight of payment and settlement systems is a central bank function whereby the objectives of safety and efficiency are promoted by monitoring existing and planned systems, assessing them against these objectives and, where necessary, inducing change’.</i></p> <p><i>In other words, ensuring that the systems are safe and efficient is an important precondition for the Eurosystem’s ability to contribute to financial stability, to implement monetary policy and to maintain public confidence in the euro.</i></p> <p><i>Furthermore, in line with the ECB’s comments on the proposed revision of the directive on payment services (PSD2), it should be noted that national supervisors and the central banks are the competent authorities to issue guidelines on incident management and incident notifications for PSPs, as well as to issue guidelines on sharing incident notifications between the relevant authorities. The recital should also take due account of the tasks conferred on the ECB by Regulation (EU) No 1024/2013.</i></p> <p><b><i>Finally, when non euroarea ESCB members perform functions equivalent to those of the Treaty and ESCB Statute tasks, under their national provisions, those functions should also not be affected.</i></b></p>	
<p style="text-align: center;">Amendment 2</p> <p style="text-align: center;">Article 1(4) and (5) (new)</p>	
<p>‘4. This Directive shall be without prejudice to</p>	<p>‘4. This Directive shall be without prejudice to</p>

<sup>2</sup> Available on the ECB’s website at [www.ecb.europa.eu](http://www.ecb.europa.eu).

<p>EU laws on cybercrime and Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection</p> <p>5. This Directive shall also be without prejudice to Directive 95/46/CE of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data<sup>3</sup>, and to Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector and to the Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data<sup>4</sup>.</p> <p>6. The sharing of information within the cooperation network under Chapter III and the notifications of NIS incidents under Article 14 may require the processing of personal data. Such processing, which is necessary to meet the objectives of public interest pursued by this Directive, shall be authorised by the Member State pursuant to Article 7 of Directive 95/46/EC and Directive 2002/58/EC, as implemented in</p>	<p><del>EU</del>ion laws on cybercrime and Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection.</p> <p><b>5. This Directive shall be without prejudice to the oversight and tasks conferred on the ECB and the ESCB concerning policies relating to the prudential supervision of credit institutions, and payment and settlement systems, for which specific risk management and security requirements have been set within the ESCB regulatory framework and that of other related Union directives and regulations. Equally this Directive shall not prejudice equivalent functions performed by ESCB members under their national frameworks.</b></p> <p>56. This Directive shall also be without prejudice to Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data<sup>3</sup> and to Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector and to the Regulation of the European Parliament and of the Council on the protection of individuals</p>
--	---

<sup>3</sup> OJ L 281, 23.11.1995, p. 31.

**ECB-PUBLIC**

<p>national law.’</p>	<p>with regard to the processing of personal data and on the free movement of such data<sup>4</sup>.</p> <p>67. The sharing of information within the cooperation network under Chapter III and the notifications of NIS incidents under Article 14 may require the processing of personal data. Such processing, which is necessary to meet the objectives of public interest pursued by this Directive, shall be authorised by the Member State pursuant to Article 7 of Directive 95/46/EC and Directive 2002/58/EC, as implemented in national law.’</p>
<p align="center"><u>Explanation</u></p> <p><i>As noted above, the ESCB has a keen interest in ensuring that payment and settlement systems function properly. This stems from the importance of payment, clearing and settlement systems for the smooth conduct of monetary policy operations and from the role they play in ensuring the stability of the financial system in general. Therefore, the ECB recommends that the proposed directive takes note of the role of the ESCB with regard to payment and settlement systems and the oversight framework already in place. The ESCB has highly effective tools to determine the safety and efficiency levels of these systems. The recital should also take due account of the tasks conferred on the ECB by Regulation (EU) No 1024/2013.</i></p> <p><i>The proposed directive should also not prejudice equivalent functions performed by non euro area ESCB members under their national frameworks.</i></p>	
<p align="center">Amendment 3</p> <p align="center">Article 6(1)</p>	
<p>‘1. Each Member State shall designate a national competent authority on the security of network and information systems (the "competent authority").’</p>	<p>‘1. Each Member State shall designate a national competent authority on the security of network and information systems (the "competent authority").’</p> <p><b>Effective cooperation shall be put in place</b></p>

<sup>4</sup> SEC(2012) 72 final.

	<p><b>between the competent authority and the European and national regulators.’</b></p>
<p style="text-align: center;"><u>Explanation</u></p> <p><i>The ECB recommends that Article 6(1) is amended in order to ensure a good level of cooperation at a Union level.</i></p>	
<p style="text-align: center;">Amendment 4</p> <p style="text-align: center;">Article 8(3)</p>	
<p>‘3. Within the cooperation network the competent authorities shall:</p> <ul style="list-style-type: none"> <li>(a) circulate early warnings on risks and incidents in accordance with Article 10;</li> <li>(b) ensure a coordinated response in accordance with Article 11;</li> <li>(c) publish on a regular basis non-confidential information on on-going early warnings and coordinated response on a common website;</li> <li>(d) jointly discuss and assess, at the request of one Member State or of the Commission, one or more national NIS strategies and national NIS cooperation plans referred to in Article 5, within the scope of this Directive.</li> <li>(e) jointly discuss and assess, at the request of a Member State or the Commission, the effectiveness of the CERTs, in particular when NIS exercises are performed at Union level;</li> <li>(f) cooperate and exchange information on all relevant matters with the European Cybercrime Center within Europol, and with other relevant European bodies in particular in the fields of data protection, energy,</li> </ul>	<p>‘3. Within the cooperation network the competent authorities shall:</p> <ul style="list-style-type: none"> <li>(a) circulate early warnings on risks and incidents in accordance with Article 10;</li> <li>(b) ensure a coordinated response in accordance with Article 11;</li> <li>(c) publish on a regular basis non-confidential information on on-going early warnings and coordinated response on a common website;</li> <li>(d) jointly discuss and assess, at the request of one Member State or of the Commission, one or more national NIS strategies and national NIS cooperation plans referred to in Article 5, within the scope of this Directive.;</li> <li>(e) jointly discuss and assess, at the request of a Member State or the Commission, the effectiveness of the CERTs, in particular when NIS exercises are performed at Union level;</li> <li>(f) cooperate and exchange information on all relevant matters with the European Cybercrime Centre<del>r</del> within Europol, and with other relevant European bodies in particular in the fields of data protection, energy, transport, banking, stock exchanges and health;</li> <li>(g) exchange information and best practices</li> </ul>

**ECB-PUBLIC**

<p>transport, banking, stock exchanges and health;</p> <p>(g) exchange information and best practices between themselves and the Commission, and assist each other in building capacity on NIS;</p> <p>(h) organise regular peer reviews on capabilities and preparedness;</p> <p>(i) organise NIS exercises at Union level and participate, as appropriate, in international NIS exercises.’</p>	<p>between themselves and the Commission, and assist each other in building capacity on NIS;</p> <p>(h) organise regular peer reviews on capabilities and preparedness;</p> <p>(i) organise NIS exercises at Union level and participate, as appropriate, in international NIS exercises.;</p> <p><b>(j) ensure the exchange of information with European and national regulators (i.e. for the financial sector: the European System of Central Banks (ESCB), the European Banking Authority (EBA) and the European Securities and Markets Authority (ESMA), which shall work closely together when security incidents are identified that could potentially impede the smooth functioning of payment and settlement systems).’</b></p>
<p align="center"><u>Explanation</u></p> <p><i>There is a strong case for sharing information with the European Network and Information Security Agency or competent authorities under the proposed directive, and with the EBA or ESMA as the competent authority for the coordination of incidents relating to PSPs.</i></p> <p><i>Hence, the ECB proposes this amendment with a view to fostering information sharing and better coordination at a Union level.</i></p>	
<p align="center">Amendment 5</p> <p align="center">Article 19(1)</p>	
<p>‘1. The Commission shall be assisted by a committee (the Network and Information Security Committee). That committee shall be a committee within the meaning of Regulation (EU) No 182/2011.’</p>	<p>‘1. The Commission shall be assisted by a committee (the Network and Information Security Committee). That committee shall be a committee within the meaning of Regulation (EU) No 182/2011.</p> <p><b>The European Central Bank (ECB), the</b></p>

**ECB-PUBLIC**

	<p><b>European Banking Authority (EBA) and the European Securities and Markets Authority (ESMA) shall be invited to send a representative to the meetings of the Network and Information Security Committee on agenda items that might have implications on the performance of the respective mandates of the ECB, EBA or ESMA.’</b></p>
<p style="text-align: center;"><u>Explanation</u></p> <p><i>The ECB has a vested interest in enhancing security in payment and settlement systems, services and instruments as an important component of maintaining confidence in the single currency and the smooth functioning of the economy in the Union. To this end, the ECB recommends that it should be invited to meetings of the NIS Committee. In any case, the ECB will have to be formally consulted under the Treaty on any such measures relating to payment systems, and any other matters falling within the ECB’s fields of competence.</i></p> <p><i>The EBA or ESMA should also be involved on issues relating to PSPs.</i></p>	